(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－286836
（P2000－286836A）
(43)公開日　平成12年10月13日(2000.10.13)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ａ	５Ｂ０５７
Ｇ０６Ｔ　1/00		Ｇ０９Ｃ　1/00	６４０Ｄ	５Ｃ０７６
Ｇ０９Ｃ　1/00	６４０		６４０Ａ	５Ｊ１０４
		Ｈ０４Ｎ　1/387		
Ｈ０４Ｎ　1/387		Ｇ０６Ｆ　15/66	Ｂ	

審査請求　未請求　請求項の数６　ＯＬ　（全　８　頁）

(21)出願番号　特願平11－88233

(22)出願日　平成11年３月30日(1999.3.30)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

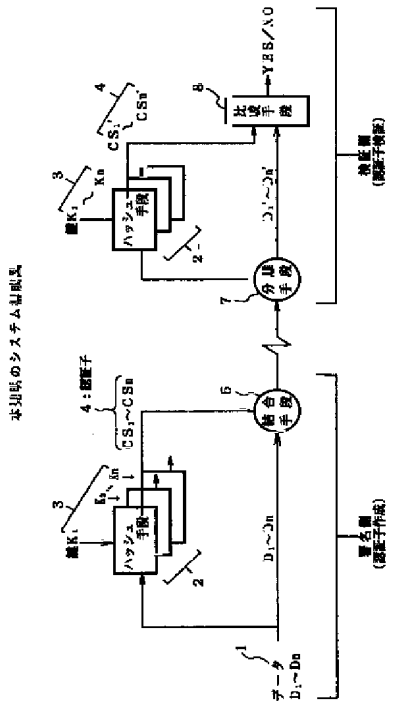
(72)発明者　小谷　誠剛
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(74)代理人　100089141
弁理士　岡田　守弘

最終頁に続く

(54)【発明の名称】　認証装置および記録媒体

(57)【要約】
【課題】 本発明は、情報を鍵を用いて一方向性の関数で認証子を作成して署名および検証する認証装置および記録媒体に関し、情報を複数に分割して異なる鍵を用いて一方向性関数でそれぞれ認証子を作成して結合などし、偽造情報作成確率を低減することを目的とする。
【解決手段】 情報を複数のデータに分割する手段と、分割した各データについてそれぞれの鍵を用いて一方向性の関数でそれぞれの認証子を作成する手段と、作成したそれぞれの認証子を情報に結合する手段とを備えるように構成する。



【特許請求の範囲】
【請求項１】情報を鍵を用いて一方向性の関数で認証子を作成して署名する認証装置において、
情報を複数のデータに分割する手段と、
上記分割した各データについてそれぞれの鍵を用いて一方向性の関数でそれぞれの認証子を作成する手段と、
上記作成したそれぞれの認証子を上記情報に結合する手段とを備えたことを特徴とする認証装置。
【請求項２】情報を鍵を用いて一方向性の関数で認証子を作成して署名する認証装置において、
情報を複数のデータに分割する手段と、
上記分割した１つのデータについて鍵を用いて一方向性の関数で認証子を作成および当該一方向性の関数で認証子を作成する際の中間の任意のデータと次のデータについて鍵を用いて一方向性の関数で認証子を作成することを繰り返す手段と、
上記作成したそれぞれの認証子を上記情報に結合する手段とを備えたことを特徴とする認証装置。
【請求項３】情報を鍵を用いて一方向性の関数で認証子を作成して検証する認証装置において、
情報からデータと認証子を分離する手段と、
上記分離した情報を複数のデータに分割する手段と、
上記分割した各データについてそれぞれの鍵を用いて一方向性の関数でそれぞれの認証子を作成する手段と、
上記作成したそれぞれの認証子および上記分離したそれぞれの認証子をもとに検証する手段とを備えたことを特徴とする認証装置。
【請求項４】情報を鍵を用いて一方向性の関数で認証子を作成して検証する認証装置において、
情報からデータと認証子を分離する手段と、
上記分離した情報を複数のデータに分割する手段と、
上記分割した１つのデータについて鍵を用いて一方向性の関数で認証子を作成および当該一方向性の関数で認証子を作成する際の中間の任意のデータと次のデータについて鍵を用いて一方向性の関数で認証子を作成することを繰り返す手段と、
上記作成したそれぞれの認証子および上記分離した認証子をもとに検証する手段とを備えたことを特徴とする認証装置。
【請求項５】情報を複数に分割する手段と、
上記分割した各データについてそれぞれの鍵を用いて一方向性の関数でそれぞれの認証子を作成する手段と、
上記作成したそれぞれの認証子を上記情報に結合する手段として機能させるプログラムを記録したコンピュータ読取可能な記録媒体。
【請求項６】情報を複数に分割する手段と、
上記分割した１つのデータについて鍵を用いて一方向性の関数で認証子を作成および当該一方向性の関数で認証子を作成する際の中間の任意のデータと次のデータについて鍵を用いて一方向性の関数で認証子を作成することを繰り返す手段と、
上記作成したそれぞれの認証子を上記情報に結合する手段として機能させるプログラムを記録したコンピュータ読取可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報を鍵を用いて一方向性の関数で認証子を作成して署名および検証する認証装置および記録媒体に関するものである。
【０００２】
【従来の技術】従来、文字、数字、記号列で作成される文書（ドキュメント）の偽造を防止するために、当該文書を所定ブロックに分割して一方向性の関数（例えばハッシュ関数）を用いて認証子を作成し、文書中の数字を他の数字に変更するというような、偽造を防止するようにしていた。
【０００３】
【発明が解決しようとする課題】しかしながら、上述した従来の一方向性の例えばハッシュ関数を用いて認証子を作成するシステムでは、偽造をより困難にするにはハッシュ関数の処理ブロック長を長くする手法が用いられていたが、十分な偽造が防止し得ないという問題があった。即ち、従来のハッシュ関数では、ＡＮＤ論理、ＯＲ論理の他四則演算子等を複雑に組み合わせて一方向性関数を実現していたが、これは経験的・直感的手法に基づいて行われ、組織的な構成法によらない。このため、従来のハッシュ関数の中には、正当なデータをハッシュ処理して得た署名データ（認証子）を不当データに改ざんして同様にハッシュ処理した結果が一致するいわゆる署名偽造が起こる問題があった。
【０００４】本発明は、これらの問題を解決するため、情報を複数に分割して異なる鍵を用い任意の信頼できる一方向性関数でそれぞれ認証子を作成して結合し、偽造情報作成確率を低減することを目的としている。
【０００５】
【課題を解決するための手段】図１を参照して課題を解決するための手段を説明する。図１において、ハッシュ手段２は、鍵を用いて一方向性の関数で認証子を作成するものである。
【０００６】結合手段５は、認証子とデータを結合するものである。分離手段７は、情報からデータと認証子とを分離するものである。比較手段８は、情報から分離した認証子と、情報から作成した認証子とを比較するものである。
【０００７】次に、動作を説明する。ハッシュ手段２が情報から分割した各データについてそれぞれの鍵３を用いて一方向性の関数でそれぞれの認証子を作成し、結合手段５が作成したそれぞれの認証子を情報に結合するようにしている。
【０００８】また、ハッシュ手段２が情報から分割した

１つのデータについて鍵３を用いて一方向性の関数で認証子を作成および一方向性の関数で認証子を作成する際の中間の任意のデータと次のデータについて鍵３を用いて一方向性の関数で認証子を作成することを繰り返し、結合手段５が作成したそれぞれの認証子を情報に結合するようにしている。

【０００９】また、分離手段７が情報からデータと認証子を分離し、ハッシュ手段２が分離された情報を複数に分割した各データについてそれぞれの鍵３を用いて一方向性の関数でそれぞれの認証子を作成し、比較手段８が作成したそれぞれの認証子および分離したそれぞれの認証子をもとに検証するようにしている。

【００１０】また、分離手段７が情報からデータと認証子を分離し、分離された情報を複数に分割した１つのデータについて鍵３を用いて一方向性の関数で認証子を作成および一方向性の関数で認証子４を作成する際の中間の任意のデータと次のデータについて鍵３用いて一方向性の関数で認証子作成することを繰り返し、比較手段８が作成したそれぞれの認証子および分離した認証子をもとに検証するようにしている。

【００１１】従って、情報を複数に分割して異なる鍵を用いて一方向性関数でそれぞれ認証子を作成して結合したり、情報から分離した認証子と情報から分離したデータを分割して異なる鍵を用いて一方向性関数でそれぞれ認証子を作成して検証したりすることにより、偽造情報作成確率を低減することが可能となる。

【００１２】

【実施例】次に、図１から図６を用いて本発明の実施の形態および動作を順次詳細に説明する。ここでは、以下、情報（テキスト、画像（静止画、動画）、音声などからなる情報）中の文（テキスト）を例に具体的に説明する（以下の具体的な説明は、例であって、画像（静止画、動画）、音声などの全てについて同様に適用できるものである）。

【００１３】図１は、本発明のシステム構成図を示す。図１において、署名側は、左側の半分によって構成され、認証子を作成して文に結合するものである。

【００１４】検証側は、右側の半分によって構成され、文から認証子を分離して文から作成した認証子とを比較して検証するものである。データ１は、文から分割したデータＤ１ないしＤｎであって、後述する図５の文（ドキュメント）中の数字、文字、記号などを所定ブロック毎に分割したデータＤ１からＤｎである。

【００１５】ハッシュ手段２は、データＤ１ないしＤｎについてそれぞれの鍵Ｋ１からＫｍを用いて一方向性の関数でそれぞれの認証子ＣＳ１からＣＳｍをそれぞれ作成するものである。

【００１６】鍵３は、認証子ＣＳ１からＣＳｍを作成するそれぞれの鍵である。認証子４は、鍵Ｋ１からＫｍによって作成されたそれぞれの認証子である。結合手段５は、作成した認証子４と、データＤ１からＤｎとを結合するものであって、後述する図５のドキュメント例に示すように、認証子４を下段に付加などするものである。

【００１７】分離手段７は、文からデータＤ１’からＤｎ’、および認証子４を分離するものである。比較手段８は、文から分離した認証子と、文から作成した認証子とを比較し、例えば一致したときに文が偽造されていなく真正と認証するものである。

【００１８】次に、図１の構成の動作を説明する。

（１）　署名側における認証子の作成：

（１－１）　文を複数に分割した入力データＤ１からＤｎ毎に、それぞれの鍵を用いてハッシュ手段２が認証子４であるＣＳ１からＣＳｍを作成する。

【００１９】（１－２）　作成されたＣＳ１からＣＳｍと、データＤ１からＤｎとを結合する。例えば後述する図５のドキュメント（文）に示すように、文章中の下段に認証子（例えば１桁４ビットからなる８桁分の認証子）を付加する。

【００２０】以上によって、文を分割したデータＤ１からＤｎ毎にそれぞれの鍵を用いて認証子ＣＳ１からＣＳｍを作成し、データＤ１からＤｎに結合することにより、文を分割したデータＤ１からＤｎ毎に異なる鍵を用いて認証子を作成することで偽造文の作成を極めて困難にし信頼性を大幅に向上させることが可能となる。

【００２１】（２）　検証側における認証子の作成：

（２－１）　（１）で作成された図５の文（ドキュメント）から認証子ＣＳ１からＣＳｍとデータＤ１’からＤｎ’を分離する。

【００２２】（２－２）　分離したデータＤ１’からＤｎ’毎に、それぞれの鍵を用いてハッシュ手段２が認証子４であるＣＳ１’からＣＳｍ’を作成する。

（２－２）　作成されたＣＳ１’からＣＳｍ’と、分離された認証子ＣＳ１からＣＳｍとを比較し、一致するか判別し、一致したときに真正の文であって偽造されていないと判定する。一方、１つでも一致しないときは偽造された文と判定する。

【００２３】以上によって、文から分離したデータＤ１からＤｎ毎にそれぞれの鍵を用いて認証子ＣＳ１’からＣＳｍ’を作成し、分離した認証子ＣＳ１からＣＳｍとを比較して全て一致したときに真正の文と判定し、１つでも不一致のときに偽造された文と判定することにより、文を分割したデータＤ１からＤｎについて異なる複数の鍵を用いて認証子をそれぞれ作成して結合することで偽造文の作成を極めて困難にし信頼性を大幅に向上させることが可能となる。以下順次詳細に説明する。

【００２４】図２は、本発明の１実施例構成図（独立多並列）を示す。これは、文を分割した入力データＤ１からＤｎについて、ｍ並列にそれぞれの鍵を用いてハッシュ手段２により認証子ＣＳ１からＣＳｍを並列に同時に作成するときの構成を示す。

【００２５】図２の（ａ）は、構成図を示す。図２の（ａ）において、入力データＤ１からＤｎは、文を分割したデータＤ１からＤｎである。

【００２６】ハッシュ手段２は、鍵Ｋを用いて認証子ＣＳを作成するものであって、ここでは、ＥＯＲ２１、一方向性関数（例えばハッシュ関数）２２およびトランケート２３から構成されるものである（図３の（ｂ）を用いて後述する）。

【００２７】ＥＯＲ２１は、排他論理和演算を実行するものであって、ここでは、データと前回の一方向性関数２２で求めた値（初回は初期値ＩＶ）との排他論理和演算を行うものである。

【００２８】一方向性関数（一方向性関数器）２２は、鍵Ｋをもとに、ＥＯＲ２１によって演算したデータから一方向性関数（例えばハッシュ関数）によって不可逆性の認証子ＣＳを作成するものである。

【００２９】トランケート２３は、一方向性関数２２によって作成された認証子ＣＳを出力するものである。出力データ（Ｄ１からＤｎ，ＣＳ１からＣＳｍ）は、入力データＤ１からＤｎについて作成した認証子ＣＳ１からＣＳｍを結合したものである（図５参照）。

【００３０】図２の（ｂ）は、認証子ＣＳの生成プロセスを示す。図２の（ｂ－１）は、ＣＳ１の生成プロセスを示す。図２の（ｂ－１）において、

① ＩＶ＝公開定数：これは、図２の（ａ）の左側から１番目のハッシュ手段２を構成するＥＯＲ２１に初期値ＩＶを設定する。

【００３１】② ＥＫ１[ＩＶ（＋）Ｄ１]＝Ｌ１１：これは、図２の（ａ）のＥＯＲ２１が① で設定した初期値ＩＶと、１番目のデータＤ１とを排他論理和演算し、その排他論理和演算した値について、一方向性関数２２が鍵Ｋ１を用いて一方向性の演算（例えばハッシュ関数によって演算）して値Ｌ１１を得る。

【００３２】③ ＥＫ１[Ｌ１１（＋）Ｄ２]＝Ｌ１２：これは、図２の（ａ）のＥＯＲ２１が② で得た値Ｌ１１と、２番目のデータＤ２とを排他論理和演算し、その排他論理和演算した値について、一方向性関数２２が鍵Ｋ１を用いて一方向性の演算（例えばハッシュ関数によって演算）して値Ｌ１２を得る。

【００３３】④ ＥＫ１[Ｌ１（ｎ－１）（＋）Ｄｎ]＝Ｌ１ｎ：これは、同様にして、図２の（ａ）のＥＯＲ２１が前回に得た値Ｌ１（ｎ－１）と、ｎ番目のデータＤｎとを排他論理和演算し、その排他論理和演算した値について、一方向性関数２２が鍵Ｋ１を用いて一方向性の演算（例えばハッシュ関数によって演算）して値Ｌ１ｎを得る。

【００３４】⑤ Ｔｒ[Ｌ１ｎ]＝ＣＳ１：これは、最後のｎ番目のデータＤｎまで終了したので、最後のｎ番目の演算結果Ｌ１ｎを認証子ＣＳ１として出力する。以上の① から⑤ の手順によって、鍵Ｋ１、初期値ＩＶを用いて認証子ＣＳ１を作成することが可能となる。

【００３５】図２の（ｂ－２）、（ｂ－３）は、図２の（ｂ－１）の① から⑤ の手順と同様に、認証子ＣＳ２，ＣＳ３を求める様子を示す。これを続けて認証子ＣＳｍを同様に求める。

【００３６】以上のように、独立にｍ並列で鍵Ｋ１からＫｍをそれぞれ用いて同時に認証子ＣＳ１からＣＳｍを算出することが可能となる。ここでは、ＣＳｍ個あたりの偽造確率＝１／2^{mP}（Ｐは認証子のビット長）となり、認証子ＣＳの数を増やすことで偽造確率を小さくすることができると共に、並列処理ができＣＳの数に依存しないで同一時間で処理可能となる。

【００３７】次に、図３を用いて図２のｍ＝３（独立３並列）の場合の構成と動作を詳細に説明する。図３は、本発明の具体例構成図（独立３並列）を示す。

【００３８】図３の（ａ）は、独立３並列の構成図を示す。これは、図２において、ｍ＝３とした場合の例であって、ハッシュ手段２、ＥＯＲ２１、一方向性関数２２、およびトランケート２３は、図２の同一番号のものと同じであるので、説明を省略する。

【００３９】図３の（ｂ）は、ハッシュ手段２におけるＣＳ１からＣＳ３の生成プロセスを示す。図３の（ｂ－１）は、図３の（ａ）の入力データＤ１からＤｎ、鍵Ｋ１，初期値ＩＶをもとに認証子ＣＳ１を作成するときの手順を示す。

【００４０】図３の（ｂ－１）において、

①’ ＩＶ＝公開定数：これは、図３の（ａ）の左側から１番目のハッシュ手段２を構成するＥＯＲ２１に初期値ＩＶを設定する。

【００４１】②’ ＥＫ１[ＩＶ（＋）Ｄ１]＝Ｌ１１：これは、図３の（ａ）のＥＯＲ２１が①’ で設定した初期値ＩＶと、１番目のデータＤ１とを排他論理和演算し、その排他論理和演算した値について、一方向性関数２２が鍵Ｋ１を用いて一方向性の演算（例えばハッシュ関数によって演算）して値Ｌ１１を得る。

【００４２】③’ ＥＫ１[Ｌ１１（＋）Ｄ２]＝Ｌ１２：これは、図３の（ａ）のＥＯＲ２１が②’ で得た値Ｌ１１と、２番目のデータＤ２とを排他論理和演算し、その排他論理和演算した値について、一方向性関数２２が鍵Ｋ１を用いて一方向性の演算（例えばハッシュ関数によって演算）して値Ｌ１２を得る。

【００４３】④’ ＥＫ１[Ｌ１（ｎ－１）（＋）Ｄｎ]＝Ｌ１ｎ：これは、同様にして、図３の（ａ）のＥＯＲ２１が前回に得た値Ｌ１（ｎ－１）と、ｎ番目のデータＤｎとを排他論理和演算し、その排他論理和演算した値について、一方向性関数２２が鍵Ｋ１を用いて一方向性の演算（例えばハッシュ関数によって演算）して値Ｌ１ｎを得る。

【００４４】⑤’ Ｔｒ[Ｌ１ｎ]＝ＣＳ１：これは、最後のｎ番目のデータＤｎまで終了したので、最後のｎ番目

の演算結果Ｌ１ｎを認証子ＣＳ１として出力する。図３の（ｂ－２）、（ｂ－３）は、図３の（ｂ－１）の⑨’から⑮’の手順と同様に、認証子ＣＳ２，ＣＳ３を求める様子を示す。

【００４５】以上の⑨’から⑮’の手順によって、独立にm並列で鍵Ｋ１からＫ３をそれぞれ用いて同時に認証子ＣＳ１からＣＳ３を算出することが可能となる。次に、図４を用いてｍ＝３で前段の中間データを次段の初期値とする場合の構成と動作を詳細に説明する。

【００４６】図４は、本発明の他の具体例構成図（ｍ＝３）を示す。図４の（ａ）は、ｍ＝３の構成図を示す。これはｍ＝３として前段の中間データを次段の初期値とした場合の例であって、ハッシュ手段２、ＥＯＲ２１、一方向性関数２２、およびトランケート２３は、図２の同一番号のものと同じ（初期値のみことなる）であるので、説明を省略する。

【００４７】図４の（ｂ）は、ハッシュ手段２におけるＣＳ１からＣＳ３の生成プロセスを示す。図４の（ｂ－１）は、図４の（ａ）の左から１番目のハッシュ手段２でＣＳ１を求める手順を示す。ここでは、既述した図３の（ｂ－１）の⑨’から⑮’と同様にしてＣＳ１を求める。

【００４８】図４の（ｂ－２）は、図４の（ａ）の左から２番目のハッシュ手段２でＣＳ２を求める手順を示す。ここでは、前段の⑮に示す中間結果（Ｌ１（ｎ－１））を初期値とし、既述した図３の（ｂ－１）の⑨’から⑮’と同様にしてＣＳ２を求める。

【００４９】図４の（ｂ－３）は、図４の（ａ）の左から３番目のハッシュ手段２でＣＳ３を求める手順を示す。ここでは、前段の⑮に示す中間結果（Ｌ２（ｎ－１））を初期値とし、既述した図３の（ｂ－１）の⑨’から⑮’と同様にしてＣＳ３を求める。

【００５０】以上の手順によって、ｍ＝３で鍵Ｋ１からＫ３をそれぞれ用いて前段の中間結果を次段の初期値として認証子ＣＳ１からＣＳ３を順次算出し、より信頼性を向上させることが可能となる。

【００５１】図５は、本発明の文の例を示す。ここでは、文（ドキュメント）は、例えば図示のように、文字、数字、記号などから構成され、これらを任意数毎にブロックに分割してデータＤ１からＤｎを作成している。また、データＤ１からＤｎよりそれぞれの鍵Ｋ１からＫｍで作成した認証子ＣＳ１からＣＳｍを結合してドキュメントの下段の特定位置に８桁（１桁４ビット）の認証子列を付加している。

【００５２】図６は、概念説明図を示す。図６の（ａ）は本発明の概念説明図を示し、図６の（ｂ）は従来技術の概念説明図を示す。

【００５３】図６の（ｂ）において、文空間Ｍは偽造対象の文の取りうる仮想的な空間であり、認証子空間は認証子の取りうる仮想的な空間である。文空間Ｍ上で偽造をより防止するには、従来では、図示のように、認証子を長ブロックにして偽造確率を小さくしていた（認証子空間上で同じ値となる、文空間Ｍ上での偽造文空間Ｍ２を点線から実線の円に示すように小さくしていた）。

【００５４】図６の（ａ）において、鍵Ｋ１を用いた場合の文空間Ｍ上での偽造文空間Ｍ１、鍵Ｋ２を用いた場合の文空間Ｍ上での偽造文空間Ｍ２、鍵Ｋ３を用いた場合の文空間Ｍ上での偽造文空間Ｍ３とすれば、本発明における鍵Ｋ１，Ｋ２，Ｋ３の３つを用いた場合には、偽造空間Ｍ１，Ｍ２，Ｍ３の共通領域である非常に小さな偽造空間Ｍ１２３となり、偽造確率を大幅に小さくすることが可能となる。

【００５５】

【発明の効果】以上説明したように、本発明によれば、情報を複数に分割して異なる鍵を用いて一方向性関数でそれぞれ認証子を作成して結合したり、情報から分離した認証子と情報から分離したデータを分割して異なる鍵を用いて一方向性関数でそれぞれ認証子を作成して検証したりする構成を採用しているため、偽造情報作成確率を簡易な手法で低減できると共に、並列処理により認証子作成時間を増やすことなく偽造情報確率を小さくしたり、前段の認証子作成時の任意の中間データを次段の初期値などとして使用することで更に偽造確率を小さくしたりできる。

【図面の簡単な説明】

【図１】本発明のシステム構成図である。

【図２】本発明の１実施例構成図（独立多並列）である。

【図３】本発明の具体例構成図（独立３並列）である。

【図４】本発明の多の具体例構成図（ｍ＝３）である。

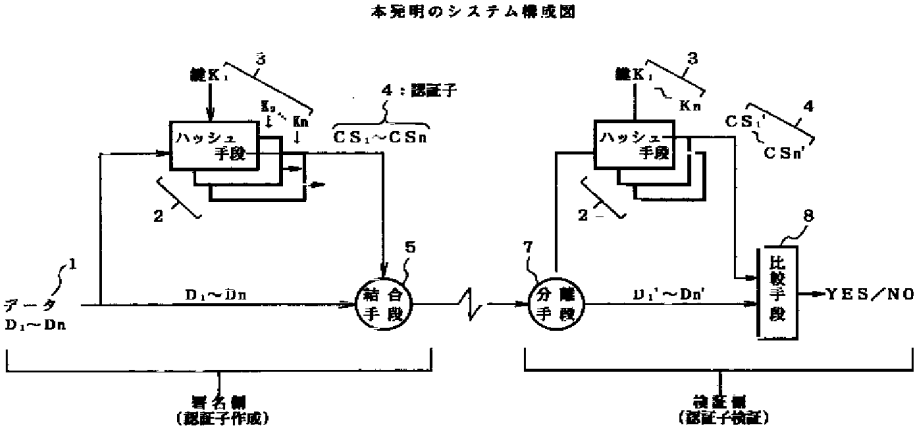
【図５】本発明の文の例である。

【図６】概念説明図である。

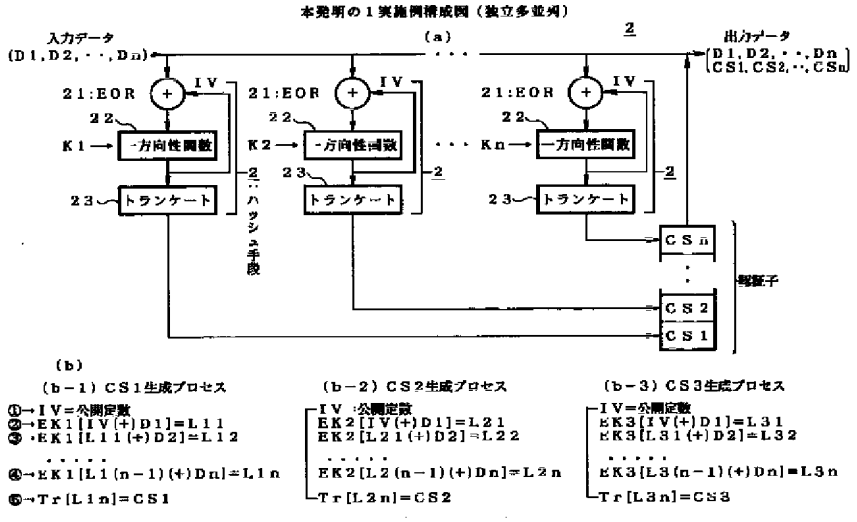
【符号の説明】

１：データ
２：ハッシュ手段
３：鍵
４：認証子
５：結合手段
７：分離手段
８：比較手段
２１：ＥＯＲ（排他論理和演算器）
２２：一方向性関数器
２３：トランケート

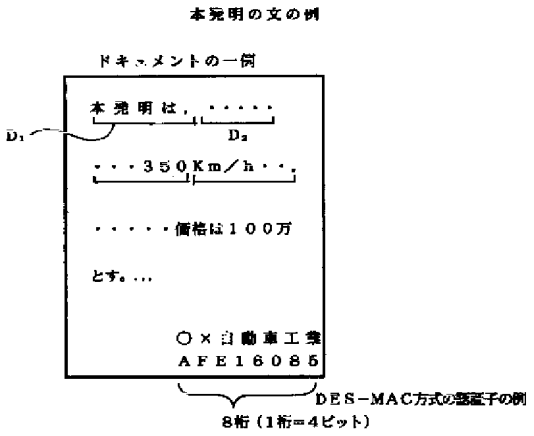
【図１】


本発明のシステム構成図
鍵K1
3
4：認証子
ハッシュ手段
CS1～CSn
2
1
データ D1～Dn
D1～Dn
結合手段
5
7
分離手段
D1'～Dn'
比較手段
8
YES/NO
署名側（認証子作成）
検証側（認証子検証）

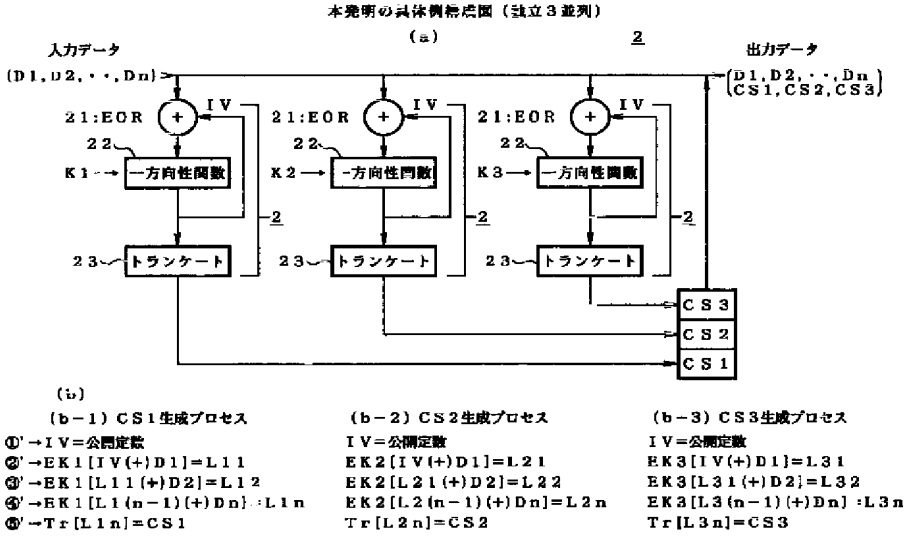
【図２】


本発明の１実施例構成図（独立多並列）
入力データ (D1,D2,・・,Dn)
出力データ (D1,D2,・・,Dn CS1,CS2,・・,CSn)
21:EOR
IV
22
K1
K2
Kn
一方向性関数
23
トランケート
2
2：ハッシュ手段
CSn
CS2
CS1
署名子
(b)
(b－1) CS1生成プロセス
①→IV=公開定数
②→EK1[IV(+)D1]=L11
③→EK1[L11(+)D2]=L12
④→EK1[L1(n-1)(+)Dn]=L1n
⑤→Tr[L1n]=CS1
(b－2) CS2生成プロセス
IV=公開定数
EK2[IV(+)D1]=L21
EK2[L21(+)D2]=L22
EK2[L2(n-1)(+)Dn]=L2n
Tr[L2n]=CS2
(b－3) CS3生成プロセス
IV=公開定数
EK3[IV(+)D1]=L31
EK3[L31(+)D2]=L32
EK3[L3(n-1)(+)Dn]=L3n
Tr[L3n]=CS3

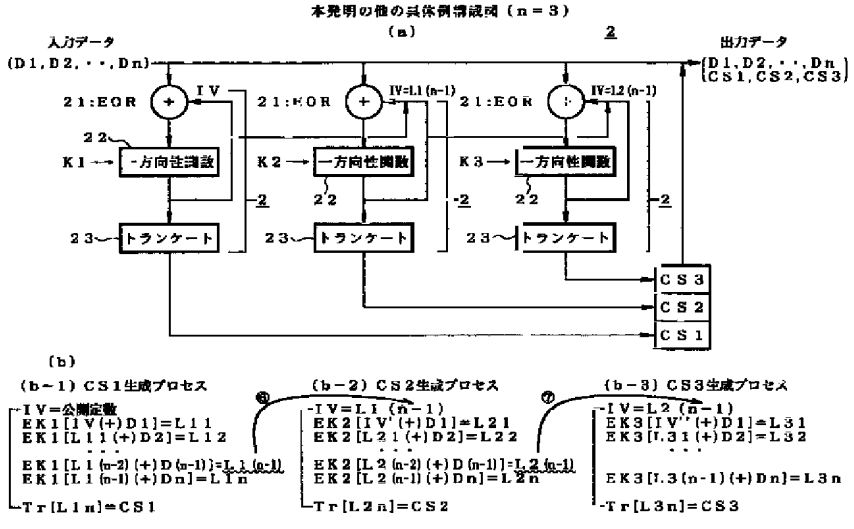
【図５】


本発明の文の例
ドキュメントの一例
本発明は，・・・・・
D1
D2
・・・350Km／h・・・
・・・・・価格は１００万
とす。…
○×自動車工業
AFE16085
DES-MAC方式の認証子の例
8桁（1桁＝4ビット）

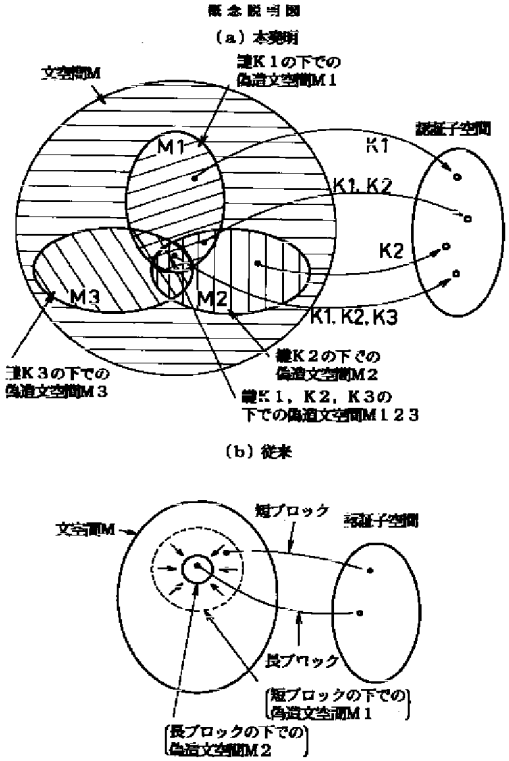
【図3】


本発明の具体例構成図（独立３並列）
(a)
入力データ
(D1,D2,・・,Dn)
出力データ
(D1,D2,・・,Dn
CS1,CS2,CS3)
21:EOR
IV
22
K1
K2
K3
一方向性関数
2
23
トランケート
CS3
CS2
CS1
(b)
(b－1) CS1生成プロセス
①'→IV＝公開定数
②'→EK1[IV(+)D1]＝L11
③'→EK1[L11(+)D2]＝L12
④'→EK1[L1(n－1)(+)Dn]＝L1n
⑤'→Tr[L1n]＝CS1
(b－2) CS2生成プロセス
IV＝公開定数
EK2[IV(+)D1]＝L21
EK2[L21(+)D2]＝L22
EK2[L2(n－1)(+)Dn]＝L2n
Tr[L2n]＝CS2
(b－3) CS3生成プロセス
IV＝公開定数
EK3[IV(+)D1]＝L31
EK3[L31(+)D2]＝L32
EK3[L3(n－1)(+)Dn]＝L3n
Tr[L3n]＝CS3

【図4】


本発明の他の具体例構成図（n＝3）
(a)
入力データ
(D1,D2,・・,Dn)
出力データ
(D1,D2,・・,Dn
CS1,CS2,CS3)
21:EOR
IV
IV=L1(n-1)
IV=L2(n-1)
22
K1
K2
K3
一方向性関数
2
23
トランケート
CS3
CS2
CS1
(b)
(b－1) CS1生成プロセス
IV＝公開定数
EK1[IV(+)D1]＝L11
EK1[L11(+)D2]＝L12
EK1[L1(n-2)(+)D(n-1)]＝L1(n-1)
EK1[L1(n-1)(+)Dn]＝L1n
Tr[L1n]＝CS1
⑥
(b－2) CS2生成プロセス
IV＝L1(n－1)
EK2[IV'(+)D1]＝L21
EK2[L21(+)D2]＝L22
EK2[L2(n-2)(+)D(n-1)]＝L2(n-1)
EK2[L2(n-1)(+)Dn]＝L2n
Tr[L2n]＝CS2
⑦
(b－3) CS3生成プロセス
IV＝L2(n－1)
EK3[IV''(+)D1]＝L31
EK3[L31(+)D2]＝L32
EK3[L3(n-1)(+)Dn]＝L3n
Tr[L3n]＝CS3

【図6】



フロントページの続き

(72)発明者　長谷部　高行
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　佐々木　孝興
東京都港区芝浦四丁目15番33号　株式会社富士通ビー・エス・シー内

Ｆターム(参考)　5B057 CA12 CA16 CB12 CB16 CC02 CE08 CG07 CH08
5C076 AA14 AA36 AA40 BA06
5J104 AA08 JA03 LA01 LA02 LA05 LA06 NA02 NA11